UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/797,715	03/08/2004	Liqun Chen	B-5394 621743-5	4135

22879 7590 07/25/2008

HEWLETT PACKARD COMPANY
P O BOX 272400, 3404 E. HARMONY ROAD
INTELLECTUAL PROPERTY ADMINISTRATION
FORT COLLINS, CO 80527-2400

EXAMINER	
SCHMIDT, KARI L	

ART UNIT	PAPER NUMBER
2139	

NOTIFICATION DATE	DELIVERY MODE
07/25/2008	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

JERRY.SHORMA@HP.COM
mkraft@hp.com
ipa.mail@hp.com

Office Action Summary	Application No.	Applicant(s)	
	10/797,715	CHEN ET AL.	
	Examiner	Art Unit	
	KARI L. SCHMIDT	2139	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *14 March 2008*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-60* is/are pending in the application.

4a) Of the above claim(s) *37-52 and 60* is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-36 and 53-59* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *08 March 2004* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *3-8-2004*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Election/Restrictions

Applicant's election without traverse to examine claims 1-36 and 53-59 drawn to key management (e.g. delegating key-provision authority), classified in class 380, subclass 277 and in the reply filed on 3/14/2008 is acknowledged. Therefore claims 37-43 and 60, drawn to trusted authority (e.g. delegating authority from a trusted authority), classified in class 713, subclass 155 and claims 44-52, drawn to access control (e.g. controlling access to a service provided by a service provider), classified in class 726, subclass 4 are withdrawn from consideration.

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

Claims 3-5, and 10, 22, 27, 33-35 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Claims 3-5 and 22

Claims 3-5 and 22 recites the limitation "said encryption" in line 1 of claim 3 and 22. There is insufficient antecedent basis for this limitation in the claim.

Claims 10 and 27

Claims 10 and 27 recites the limitation "second key pair" in line 2 and 5 of claim 10 and 27. There is insufficient antecedent basis for this limitation in the claim. Further the examiner notes the “second key pair” is indefinite due to the face that it is never mentioned in claim 1 and 19, therefore the examiner is confused on what the second key pair actually is? Is it related to the starting key pair or its own generated key pair? The examiner will interpret the “second key pair” to be the starting key that is approved by the trusted authority.

Claims 33-35

Claims 33-35 recites the limitation "service provider". There is insufficient antecedent basis for this limitation in the claim.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

Claims 1-36 and 53-59 rejected under 35 U.S.C. 102(e) as being anticipated by Appenzeller et al. (US 2004/0098589 A1).

Claim 1

Appenzeller claims a method of delegating key-provision authority to a device from a trusted authority, the method comprising providing a yet-to-be completed chain of public/private cryptographic key pairs linked in a subversion-resistant manner (see at least, Abstract: the examiner notes using an IBE and identity information to have private key generator to generate keys based on the public parameters of the user) and comprising: a starting key pair formed by a public/private key pair of the trusted authority (see at least, [0041]: the examiner notes the master secret S (e.g. secret master key) can be produce off site (e.g. trusted authority and is sent to the PKG), a penultimate key pair formed by public/private data, the private data being securely stored in the device for access only under circumstances that have been pre-authorised by the trusted authority and comprise a specific key-generation process running in a subversion-resistant operating environment (see at least, [0066]: the examiner notes a public key can identify the receiver and further the receiver has public parameter information P and SP that maybe shared between a large number of potential recipients), and a link between the penultimate key pair and an end key pair to be formed by an encryption/decryption key pair of an Identifier-Based Encryption, IBE, scheme; this link being said key-generation process arranged to execute in said subversion-resistant operating environment on the device to generate said decryption key using said private data and the IBE encryption key and to make the generated key available for use (see at least, [0039]: the examiner notes an identity based encryption scheme in which private keys(e.g. see [0047]) maybe generated based on the identities

of the users and [0057] and [0065]: the examiner notes the receivers equipment uses values of the private key for decryption).

Claims 2 and 20

Appenzeller discloses a method according to claim 1, wherein said key-generation process is arranged to check that at least one condition has been satisfied before the process generates the decryption key and/or makes the key available for use (see at least, [0050]: the examiner notes authentication is a form of a condition that must be satisfied before the private key generate a private key).

Claims 3, 21 and 54

Appenzeller discloses a method according to claim 2, wherein said at least one condition comprises a condition to be presented to the device in said encryption key (see at least, [0050]: the examiner notes a biometric identification represents a condition that is presented to the device).

Claims 4 and 22

Appenzeller discloses a method according to claim 3, wherein said condition indicated in said encryption key is a condition that is to be met by particular data stored in the device, this data having been provided by the trusted authority and stored in the device protected against subversion (see at least, [0051]: the examiner notes the private key

maybe contain on a computer readable medium and the user must pass authentication as a condition (e.g. see [0050]).

Claims 5, 23 and 55

Appenzeller discloses a method according to claim 3, wherein said condition indicated in said encryption key is a condition that is to be satisfied by input data presented by a user of the device (see at least, [0050]: the examiner notes a biometric identification represents a condition that is presented to the device).

Claims 6 and 25

Appenzeller discloses a method according to claim 2, wherein said at least one condition comprises a condition to be presented in encrypted form to the device (see at least, [0042]: the examiner notes the PKG used the master secret S (e.g. secret master key and “a condition presented in encrypted form”).

Claims 7, 24 and 56

Appenzeller discloses a method according to claim 2, wherein said at least one condition comprises a condition that input data presented by a user of the device has a predetermined relationship with particular data stored in the device and protected against subversion (see at least, [0044]: the examiner notes the public parameters P and sP can be pre installed in software for the user equipment).

Claim 8

Appenzeller discloses a method according to claim 7, wherein said at least one condition is a user authentication condition concerning a current user of the device (see at least, [0050]: the examiner notes a biometric identification represents a condition that is presented to the device).

Claims 9, 26 and 58

Appenzeller discloses a method according to claim 1, wherein said penultimate key pair is the second key pair in said chain, the start key pair and penultimate key pair being linked by said public data being certified by the trusted authority, using its private key, to indicate that an entity holding the corresponding said private data is one to which it has delegated authority (see at least, [0041]: the examiner notes the master secret S (e.g. secret master key) is the first key used and further the PKG holds the public data P and sP (e.g. see [0042]) in which the PKG acts as the delegated authority, and [0066]: the examiner notes a public key (e.g. penultimate key pair) acts as the second key pair in the chain).

Claims 10 and 27

Appenzeller discloses a method according to claim 1, wherein said penultimate key pair is the third key pair in said chain, the private key of the second key pair being securely stored in the device, and the start key pair and the second key pair being linked by the public key of the second key pair being certified by the trusted authority, using its private

key, to indicate that an entity holding the private key of the second key pair is one to which it has delegated authority; the second key pair being linked to the penultimate key pair by said key-generation process being arranged to be activated in order to respond to a challenge based on the public key of the second key pair before attempting to complete said chain by providing said decryption key (see at least, [0041]: the examiner notes the master secret S (e.g. secret master key) is the first key used and further the PKG holds the public data P and sP (e.g. see [0042]) in which the PKG acts as the delegated authority, and [0066]: the examiner notes a public key (e.g. penultimate key pair) acts as the second key pair in the chain).

Claims 11 and 28

Appenzeller discloses a method according to claim 1, wherein the private key of at least one key pair of said chain, additional to the first key pair, is held outside said device (see at least, [0064]: the examiner notes private key generator will provide the receiver the private key over a trusted communication path (e.g. outside of the device)).

Claims 12 and 29

Appenzeller discloses a method according to claim 1, wherein the or each link in at least the portion of the chain extending from the starting key pair to the penultimate key pair is verifiable by a party wishing to rely on the delegation of authority to the device from the trusted authority (see at least, [0080]: the examiner notes the certificate authority authentication the private key generator and thereby would delegate authority).

Claims 13 and 30

Appenzeller discloses a method according to claim 12, wherein at least one of the verifiable links is verifiable as a result of the public key of the downstream key pair associated with the link being certified using the private key of the upstream key pair associated with that link (see at least, [0080]: the examiner notes the certificate authority authentication the private key generator and thereby would delegate authority and [0047]: the examiner notes the private key generator generates private keys for the users, further the examiner notes that this is a verifiable link for the (see at least, [0080]: the examiner notes the certificate authority authentication the private key generator and thereby would delegate authority).downstream/upstream key pair due to the fact that the CA authenticates the PKG and the PKG authenticates the user).

Claims 14 and 31-32

Appenzeller discloses a method according to claim 1, wherein the device comprises a trusted platform arranged to execute the key-generation process in said subversion-resistant operating environment (see at least, [0041]: the examiner notes the PKG generating a private key).

Claim 15

Appenzeller discloses a method according to claim 14, wherein the trusted authority checks the trusted platform status of the device (see at least, [0080]: the examiner

notes the certificate authority authentication the private key generator and thereby would delegate authority).

Claims 16 and 59

Appenzeller discloses a method according to claim 14, wherein said public data is held in protected storage and only accessible by the key-generation process when executing in said subversion-resistant operating environment (see at least, [0042]: the examiner notes the PKG uses the master secret S and public parameter P to generate a private key).

Claims 17, 36 and 57

Appenzeller discloses method according to claim 4, wherein the device comprises a trusted platform arranged to execute the key-generation process in said subversion-resistant operating environment, said public data and said particular data being held in protected storage and only accessible by the key-generation process when executing in said subversion-resistant operating environment (see at least, [0042]: the examiner notes the PKG uses the master secret S and public parameter P to generate a private key).

Claim 18

Appenzeller discloses a method according to claim 17, wherein said particular data is profile data for a party associated with the device (see at least, [0047]: the examiner notes the user identity may contain email address, name, etc).

Claims 19 and 53

Appenzeller discloses a data access control method involving delegated authority, the method comprising: attempting to complete a chain of public/private cryptographic key pairs linked in a subversion-resistant manner (see at least, Abstract: the examiner notes using an IBE and identity information to have private key generator to generate keys based on the public parameters of the user) and comprising: a starting key pair formed by a public/private key pair of a trusted authority (see at least, [0041]: the examiner notes the master secret S (e.g. secret master key) can be produce off site (e.g. trusted authority and is sent to the PKG), a penultimate key pair formed by public/private data, the private data being securely stored in a device for access under circumstances that have been pre-authorised by the trusted authority and comprise a specific key-generation process running in a subversion-resistant operating environment (see at least, [0066]: the examiner notes a public key can identify the receiver and further the receiver has public parameter information P and SP that maybe shared between a large number of potential recipients), and a link between the penultimate key pair and an end key pair to be formed by an encryption/decryption key pair of an Identifier-Based Cryptographic, IBE, scheme; this link being said key-generation process arranged to

execute in said subversion-resistant operating environment on the device to provide the IBE decryption key, generated using said private data and the IBE encryption key (see at least, [0039]: the examiner notes an identity based encryption scheme in which private keys(e.g. see [0047]) maybe generated based on the identities of the users and [0057] and [0065]: the examiner notes the receivers equipment uses values of the private key for decryption), attempted completion of said chain being effected by executing said key-generation process in said subversion-resistant operating environment on the device; and where execution of the key-generation process results in the provision of the decryption key, using the decryption key to decrypt data encrypted using said public data and said IBE encryption key (see at least, [0050]: the examiner notes authentication is a form of a condition that must be satisfied before the private key generate a private key).

Claim 33

Appenzeller discloses a method according to claim 19, wherein the encrypted data is data encrypted by a service provider, decryption of the encrypted data being required in order to gain access to a service provided by the service provider (see at least, [0053]: the examiner notes a sender encrypts a message and sends it to a receiver who is require to decrypt the message).

Claim 34

Appenzeller discloses a method according to claim 33, wherein the encrypted data provided by the service provider is a data component of the service (see at least, [0070]: the examiner notes the users can be subscribers to a particular service and [0072]: a sender sends an encrypted message to the receiver).

Claim 35

Appenzeller discloses a method according to claim 33, wherein the encrypted data provided by the service provider is arbitrary data, the method further comprising returning the decrypted data to the service provider as evidence that said conditions have been met, and the service provider thereafter providing said service to the party (see at least, [0069]: the examiner notes the secure exchange messages between sender and receiver can contain commands, data, ...etc).

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to KARI L. SCHMIDT whose telephone number is (571)270-1385. The examiner can normally be reached on Monday - Friday: 7:30am - 5:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kristine Kincaid can be reached on 571-272-4063. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Kari L Schmidt/
Examiner, Art Unit 2139

/Kristine Kincaid/
Supervisory Patent Examiner, Art Unit 2139